UNITED STATES MARINE CORPS
MARINE CORPS INSTALLATIONS COMMAND
3000 MARINE CORPS PENTAGON
WASHINGTON, DC 20350-3000

MCICOMO 3000.1
G-3/5/7
JUN 29 2015

MARINE CORPS INSTALLATIONS COMMAND ORDER 3000.1

From: Commander, Marine Corps Installations Command
To: Distribution List

Subj: INSTALLATION PROTECTION

Ref: (a) MCO 5400.54 MCICOM Roles and Responsibilities
        (b) MARADMIN 597/12 MCICOM and TECOM Responsibilities in
            the USNORTHCOM and USPACOM Areas of Responsibility
            for USMC AT Program and FP Responsibilities 17 Oct
            2012
        (c) MARFORPAC/I&L Memorandum of Understanding 23 Jul 2013
        (d) MCO 3058.1 Marine Corps Mission Assurance
        (e) Charter for the USMC Mission Assurance Operational
            Advisory Group Charter, November 2012
        (f) MCO 3440.9 Marine Corps IEM Program
        (g) USMC HHQ Mission Assurance Program Review Benchmarks
            (SEC)
        (h) DoD 8910.1-M Procedures for Management of Information
            Requirements
        (i) MARADMIN 036/13 Green Team Study - Capability
            Portfolio Management
        (j) MCO 3302.1E USMC AT Program
        (k) SECNAV 5510.30 CEP
        (l) DODI 6055.17 IEM Program
        (m) OPORD #01022013 - Development of COLS in Support of
            POM 2016
        (n) I&L Charter for the Marine Corps Installations &
            Logistics Advocacy Process, May 2013
        (o) USMC Protection Advocate Charter, June 2013
        (p) DODI 2000.16E DoD AT Standards
        (q) MARADMIN 618-12 Implementation of MCCAMS-NG
        (r) MCO 5580.2B Ch_1 Law Enforcement Manual
        (s) MCO 5500.6H Arming of Law Enforcement and Security
            Personnel and the Use of Force
        (t) USMC SEC Mission Assurance Benchmarks
        (u) MCO 5530.14A Marine Corps Physical Security Program
            Manual
        (v) DoD Manual 5100.76 Physical Security of Conventional

          Arms, Ammunition, and Explosives
     (w) DoD Reg 5200.08-R Physical Security Program
     (x) NAVMC 3500.103 USMC AT Manual
     (y) MCICOMO 3030.1 Marine Corps Installations Command
          Continuity of Operations Program 3 Sep 14
     (z) DODI 6055.17 Pandemic Influenza Response Plan
     (aa) MCO 3501.36A Marine Corps CIP
     (ab) MCO 11000.11 Marine Corps Fire Protection and
          Emergency Services Program
     (ac) CFAI F&ES Self-Assessment and Accreditation Program,
          August 2011
     (ad) MCO 3440.8 Installation CBRNE Protection Program
     (ae) DODI 3020.52 DoD Installation CBRNE Preparedness
          Standards
     (af) MCO 1620.2D Armed Force Disciplinary Control Board

Encl: (1) Resource Management
       (2) Mission Assurance
       (3) Law Enforcement
       (4) Physical Security
       (5) Antiterrorism
       (6) Installation Emergency Management
       (7) Critical Infrastructure Protection
       (8) Emergency Dispatch Services
       (9) Fire and Emergency Services
       (10) Installation Chemical, Biological, Radiological,
            Nuclear and Explosive Protection

1. Situation

   a. General

        (1) In accordance with reference (a), Marine Corps
Installations Command (MCICOM) was established by a Commandant
of the Marine Corps-directed reorganization of the Installations
and Logistics (I&L) Department, Headquarters Marine Corps. The
primary goal of MCICOM is to enhance base and station support to
the Marine Corps warfighting mission.

        (2) MCICOM defines Installation Protection (IP) as the
preservation of the effectiveness and survivability of mission-
related military and non-military personnel, equipment,
facilities, information, and infrastructure located within or in
direct support of a Marine Corps base, station or facility.
MCICOM uses the IP capability portfolio as the framework to
organize, manage, and resource the protection-related programs
of Law Enforcement (LE); Physical Security (PS); Antiterrorism

(AT); Installation Emergency Management (IEM); Critical Infrastructure Protection (CIP); Emergency Management Communications including Emergency Dispatch Services (EDS); Fire and Emergency Services (F&ES); and Installation Chemical, Biological, Radiological, Nuclear, High-Yield Explosive (CBRNE) Protection; to include all related sub-functions and activities.

(3) Per reference (a), MCICOM exercises command and control of the Marine Corps Installations (MCI) regional commands and provides oversight, direction, and coordination of base and station services and support for all bases and stations. The regional MCI Commanding Generals report to Commander, MCICOM (COMMCICOM).

(4) Per references (b) and (c) MCICOM interfaces with Marine Forces North (MARFORNORTH) and Marine Forces Pacific (MARFORPAC) in supporting/supported relationships to ensure effective support to U.S. Northern Command (USNORTHCOM) and U.S. Pacific Command (USPACOM) in the execution of their antiterrorism and force protection responsibilities.

(5) Per reference (a), U.S. Marine Corps Forces Command (MARFORCOM) interfaces with MCICOM through a Supported/Supporting relationship for Force Protection at USMC installations where MARFORCOM subordinate units are tenants.

b. Enemy

(1) Threats and hazards to bases, stations, and personnel stem from a variety of sources. These threats and hazards include, but are not limited to, traditional physical attack, cyber intrusions, and man-made and natural disasters.

(2) Terrorist groups continue to pursue their traditional goals of generating publicity and instilling panic while developing new methods and capabilities of attack intended to achieve maximum publicity, inflict injuries to personnel, damage infrastructure and critical assets, and alter our way of life.

c. Friendly

(1) Adjacent

(a) Marine Forces Command (MARFORCOM)

(b) Marine Forces Pacific (MARFORPAC)

(c) Marine Forces North (MARFORNORTH)

(d) Marine Forces Reserve (MARFORRES)

(e) Marine Corps Logistics Command (LOGCOM)

(f) Marine Corps Combat Development Command/Training & Education Command (MCCDC/TECOM)

(g) Defense Logistics Agency (DLA)

(h) Commander, Navy Installations Command (CNIC)

(i) U.S. Navy Bureau of Medicine and Surgery (BUMED)

(2) Subordinate

(a) Marine Corps Installations East-Marine Corps Base Camp Lejeune (MCIEAST-MCB CAMLEJ)

(b) Marine Corps Installations West-Marine Corps Base Camp Pendleton (MCIWEST-MCB CAMPEN)

(c) Marine Corps Installations Pacific-Marine Corps Base Camp Butler (MCIPAC-MCBCB)

(d) Marine Corps Installations National Capital Region-Marine Corps Base Quantico (MCINCR-MCBQ)

(3) Supporting Commands and Agencies

(a) Emergency Management and response agencies from local/state/federal/non-governmental organizations (NGOs) and host nations. These groups provide key support for bases and stations in the execution of their mission essential tasks.

(b) Tenants on MCICOM bases and stations. Tenants will integrate their protection plans with the host IP plan.

d. Applicability. This Order is applicable to MCICOM HQ, MCIEAST-MCB CAMLEJ, MCIWEST-MCB CAMPEN, MCIPAC-MCBCB, and MCINCR-MCBQ.

2. Mission. Provide policy and guidance for implementing IP at MCICOM Headquarters (HQ) and regions in order to maintain the mission capability, operational readiness, and quality of life

of Marine Corps organizations and personnel aboard bases and stations.

3. Execution

   a. Commander's Intent

      (1) Purpose. Provide policy and guidance for IP at MCICOM HQ and regions that shapes and defines IP organizational roles and responsibilities, improves program management, implements the Mission Assurance-Risk Management Process (MA-RMP), and further aligns program management efforts to the installation advisory group/advocacy construct.

      (2) Method. The Commander's intent will be accomplished by building upon existing capabilities and improving efficiency through: functionally aligning and balancing the IP organizational structure at HQ and regions, ensuring HQ and regional Program Managers are trained and actively operating off of standard programming and execution guidance, institutionalizing the use of the MA-RMP, and presenting IP resource requirements to the advocacy boards to address identified risks.

      (3) Endstate. MCICOM HQ, MCIEAST-MCB CAMLEJ, MCIWEST-MCB CAMPEN, MCIPAC-MCBCB, and MCINCR-MCBQ are commonly and effectively organized, staffed, trained, and equipped to complete assigned program management and protection functions in order to ensure operational readiness and to protect life and property aboard all Marine Corps bases and stations.

   b. Concept of Operations. MCICOM HQ will provide policy, guidance, and conduct resource management activities to manage an effective IP capability portfolio. Unless otherwise directed by this Order, regional commands will continue to carry out their IP-related responsibilities as published in their standing orders and directives. Concurrently, the following objectives will be met.

      (1) Objectives

         (a) Organization. Functionally align and balance the IP organizational structure by establishing an IP Branch within the G-3 division at MCICOM HQ, MCIEAST, MCIWEST, MCIPAC, and MCINCR responsible for management and oversight of the eight primary programs as depicted in enclosure (1). The IP Branch

will be organized and staffed to complete the following tasks within respective AoRs:

      <u>1</u>. Serve as the Office of Primary Responsibility (OPR) for all IP-related matters.

      <u>2</u>. Provide Subject Matter Expertise (SME) for IP matters, establish policy, and publish guidance for the subordinate elements.

      <u>3</u>. Develop and maintain expert capability for Planning, Programming, Budgeting, and Execution (PPBE) activities for IP Capability Portfolio Management (CPM).

      <u>4</u>. Provide oversight and assessment of subordinate elements.

      (b) <u>Implementation of IP CPM</u>. Ensure full implementation of all IP capability portfolio program functions, sub-functions, and activities through legally published guidance, effective oversight and resource management.

      (c) <u>Execute the MA-RMP</u>. Per reference (d), use the MA-RMP process to: (1) ensure mission owners' and asset owners' protection efforts are coordinated, (2) link risk management (RM) activities across the IP capability portfolio, and (3) support prioritization of effort and resources across the IP capability portfolio.

  c. <u>Tasks</u>

    (1) <u>Assistant Chief of Staff (AC/S), G-1, MCICOM</u>

      (a) Provide representation to the Installation Protection Capability Portfolio Review Board (IP CPRB) and subordinate working groups (WGs) as requested by MCICOM G-3.

      (b) Support development of Table of Organization changes and other administrative actions for the new G-3 IP Branches that will reside at MCICOM HQ and all regional commands.

      (c) Provide support and expertise on personnel and administrative issues that impact the planning and execution of COMMCICOM's IP mission.

    (2) <u>AC/S, G-3/5/7, MCICOM</u>

(a) Develop, execute, and maintain MCICOM IP policy and guidance.

(b) Establish an IP Branch within the G-3 division with three (3) subordinate sections consistent with enclosure (1). The IP Branch will be responsible for managing the IP capability portfolio, which consists of the following eight protection-related programs: Law Enforcement (LE), Physical Security (PS), Antiterrorism (AT), Installation Emergency Management (IEM), Critical Infrastructure Protection (CIP), Emergency Management Communications including Emergency Dispatch Services (EDS), Fire and Emergency Services (F&ES), and Installation Chemical, Biological, Radiological, Nuclear, High-Yield Explosive (CBRNE) Protection, to include all related sub-functions and activities.

(c) Charter and chair the IP CPRB and subordinate WGs. Maintain meeting minutes as required by the applicable references.

(d) Designate in writing the command's Director of IP.

(e) Designate in writing the command's Program Manager(s) with lead responsibility for the eight programs identified in enclosure (1).

(f) Per reference (e), provide an O-6/GS-15 level representative to the Deputy Commandant, Plans, Policies, and Operations (DC, PP&O)-chartered MA Operational Advisory Group. Ensure appropriate level representation to all of the chartered protection-related advocacy boards.

(g) Develop and maintain an Emergency Management Plan (EMP) for MCICOM HQ.

(h) Coordinate and publish the command's all-hazards & threat (AH&T)-based exercise program plan per reference (f).

(i) Monitor threat levels and implement FPCONs to meet known threats and/or as directed by MARFORPAC and MARFORNORTH for their Areas of Responsibility (AORs).

(j) In accordance with references (d) and (g), complete an annual Program Review (PR) (self-assessment) and be prepared for an onsite assessment by external commands every third year.

(k) Coordinate and/or conduct all program reviews over subordinate commands as required. Every third year complete an onsite review of subordinate commands using reference (g) and provide corrective action assistance as necessary.

(l) Establish or participate in a Threat Working Group (TWG) to collaborate and share relevant threat information with all appropriate stakeholders.

(m) Ensure MCICOM subordinate commands implement risk management procedures per references (d), (f), and enclosure (2).

(n) Review regional command quarterly Defense Readiness Reporting System (DRRS) reports for Marine Corps Task (MCT) 6.0 (Protect the Force). Provide adjacent/supported commands amplifying information when requested.

(o) Provide guidance and oversight to make sure contracts are written that ensure the continuous and uninterrupted production/procurement and delivery of the required level of critical asset supporting materiel and services. This should include consideration of transport and security of the materiel and services, contractor support obligations, and source of materiel and services, including foreign and domestic partners.

(p) Provide guidance and oversight to ensure all contracts are written to incorporate AT requirements.

(3) AC/S, G-4, MCICOM

(a) Provide representation to the IP CPRB and subordinate WGs as requested by MCICOM G-3.

(b) Provide support and expertise on logistical issues that impact the planning and execution of COMMCICOM's IP mission.

(4) AC/S, G-6, MCICOM

(a) Provide representation to the IP CPRB and subordinate WGs as requested by MCICOM G-3.

(b) Coordinate and maintain daily status of Network and Communication services operational conditions (NETOPS) in

response to threats and attacks that affect the command's IP Information Environment as appropriate per with reference (h).

(c) Ensure coordination and integration of cybersecurity efforts within the IP Portfolio.

(d) Provide SME support and coordinate C4 support requirements generated by this Order.

(5) AC/S, G-8, MCICOM

(a) Provide representation to the IP CPRB and subordinate WGs as requested by MCICOM G-3.

(b) In coordination with MCICOM G-3, implement annual procedures to incorporate mission assurance assessment (MAA) data to assist in prioritizing current year deficiency (CYD) requests and to inform annual Program Objective Memorandum (POM) guidance.

(c) Support the development of the IP capability portfolio within the Installations Program Evaluation Board (INS PEB) per reference (i) and enclosure (1).

(d) Provide support and expertise on resource management issues that impact the planning and execution of COMMCICOM's IP mission.

(6) AC/S, G-F, MCICOM

(a) Provide representation to the IP CPRB and subordinate WGs as requested by MCICOM G-3.

(b) Provide support and expertise on the execution of all facilities and environmental related issues that impact the planning and execution of COMMCICOM's IP mission.

(c) In coordination with MCICOM G-3, implement annual procedures to incorporate MAA data into project prioritization for Military Construction and Facilities Sustainment, Restoration, and Modernization programs.

(7) Staff Judge Advocate (SJA), MCICOM

(a) Provide representation to the IP CPRB and subordinate WGs as requested by MCICOM G-3.

(b) Provide support and expertise on legal issues that impact the planning and execution of COMMCICOM's IP policy.

(8) Public Affairs Officer, MCICOM

(a) Provide representation to the IP CPRB and subordinate WGs as requested by MCICOM G-3.

(b) Coordinate press releases and media queries concerning IP matters.

(c) Provide support and expertise on all public affairs issues that impact the planning and execution COMMCICOM's IP mission.

(9) Security Manager, MCICOM

(a) Provide representation to the IP CPRB and subordinate WGs as requested by MCICOM G-3.

(b) Support the identification and prioritization of MCICOM HQ facilities' classified material handling/storage and other supporting infrastructure.

(c) Ensure all MCICOM official travelers comply with the Foreign Clearance Guide. Ensure compliance with in-transit security and force tracking requirements per reference (j). All travelers shall receive country-specific threat briefs.

(d) Provide support and expertise on all personnel security and information security issues that impact the planning and execution of COMMCICOM's IP mission, to include the command's Continuous Evaluation Program per reference (k).

(10) Director of Safety, MCICOM

(a) Provide representation to the IP CPRB and subordinate WGs as requested by MCICOM G-3.

(b) Provide support and expertise on safety and occupational health issues that impact the planning and execution of COMMCICOM's IP Program.

(c) Coordinate with the Director, Health Services, HQMC, to ensure command health and medical sector issues/ activities are identified and addressed in support of the command's IEM program.

(11) <u>Commanding Generals, Marine Corps Installations Pacific, West, East, and National Capital Region</u>. MCI regional commanders are responsible for IP capability portfolio management, including the collective oversight and management of installation-level IP programs. The regional G-3 IP Branch personnel serve as SMEs and program managers. Regional commands shall:

(a) Employ this Order's three main objectives to inform and guide the execution of IP within respective AORs.

(b) Publish guidance for IP that integrates protection-related programs and requirements, implements program management guidance consistent with the enclosures, executes the required risk management process, and achieves the stated objectives and endstate of this order.

(c) Establish an IP Branch within the G-3 division that is manned, trained, and equipped to manage the IP capability portfolio in accordance with enclosure (1).

(d) Designate in writing a Director of IP for the command.

(e) Designate in writing the command's Program Manager(s) with lead responsibility for the eight programs identified in enclosure (1).

(f) Plan and execute an AH&T-based exercise program consistent with references (f), (j), (l), (p), (aa), and (ae). Include this exercise program as a part of an annual Training, Exercise, Engagement, and Employment Plan (TEEEP) submission to MCICOM's G3/5/7 Branch by the middle of third quarter fiscal year (Q3FY).

(g) Per references (d) and (g), conduct, and ensure subordinate installations complete, annual self-assessments using Mission Assurance Assessment (MAA) benchmarks and the enterprise Mission Assurance Assessment Tool (eMAAT). These are the minimum standards for evaluation. Commanders may exceed these requirements. To reduce redundancy, self-assessments will not be conducted on any base or station during the year in which it receives a HQMC MAA. In support of the HQMC MAA, ensure subordinate installations upload required documents requested by the MAA Team to SharePoint in advance of HQMC MAA. SharePoint site is located at the following address:

https://ehqmc.usmc.mil/org/hqmcppo/PS/PSM/MAATInstallations/default.aspx.

(h) Review and update all IP-related plans annually or as required by higher headquarters (HHQ) policy and guidance.

(i) Establish an Information Fusion capability to monitor threat levels and facilitate the collection and timely dissemination of threat assessments, indications, and warnings to and from subordinate bases and stations. Implement FPCONs to meet known threats and/or as directed.

(j) At a minimum, establish the following forums, which meet at least quarterly unless otherwise required or directed by Marine Corps policy:

<u>1</u>. Mission Assurance Executive Council (MAEC) and Mission Assurance Working Group (MAWG). (Command MAWGs report up to MCICOM's IP CPRB.)

<u>2</u>. Functional Area Working Groups as required (e.g., ATWG, CIPWG, F&ESWG, EMWG, etc.). These working groups may be combined, as needed.

<u>3</u>. Regional TWG.

(k) Use enclosure (1) to guide resource management activities for IP-related resources in annual PPBE activities in order to provide effective program management and oversight necessary to establish, maintain, and execute IP.

<u>1</u>. Take necessary actions to manage IP capabilities and resources as a portfolio to meet the intent of reference (g).

<u>2</u>. Per reference (k), support development and implementation of Common Output Levels of Service (COLS) to measure and assess risk associated with resourcing levels and prepare effective, informed, and capabilities-based POM initiatives.

<u>3</u>. Adhere to programming guidance provided by MCICOM G-8 for use of IP-related Marine Corps Program Codes (MCPCs) in support of a logical and defendable resource portfolio.

4. Focus on use of IEM Program standards and guidance to: better align efforts with industry standards and best practices; synchronize IEM activities with all external stakeholders (local, state, tribal, federal, private sector, and non-governmental organizations) before, during, and after emergencies; remove redundancies within the IP capability portfolio programs (i.e. plan development, exercises, etc.), and consolidate resource requirements for these activities under a single program manager for IEM as depicted in enclosure (1).

5. Align advocacy efforts to the frameworks established by the Installations Advocate (Deputy Commandant, Installations and Logistics (DC, I&L)) and the Protection Advocate (DC, PP&O) per references (n) and (o).

(l) Commanders shall establish guidance for off-base and station facilities, housing, transportation services, daycare centers, and other activities used by or involving a mass gathering of DOD personnel and their dependent family members per reference (p).

(m) Provide representation to the IP CPRB and subordinate WGs requested by MCICOM G-3. The IP CPRB fulfills the MCICOM MAWG requirement and supports DC, I&L and DC, PP&O in their advocacy forums.

d. Coordinating Instructions

(1) Per paragraph 3.c., regions shall submit a list of command appointed IP-related points of contact (POCs) and update annually on 1 October to MCICOM's IP Branch.

(2) Regional commands submit a consolidated TEEEP to MCICOM's G3/5/7 to include AH&T-based training and exercises annually by 15 May.

(3) Submit regional command annual PR (self-assessment) as required by the applicable references. These assessments will be completed no later than 31 December of each year and submitted to MCICOM's IP Branch upon completion.

(4) Provide all supported commands with IP-related data and Mitigation Action Plans (MAPs) when requested.

(5) Regional IP Branches shall brief changes to their region's quarterly DRRS report for MCT 6.0 (Protect the Force) during the quarterly IP CPRB meetings.

4. Administration and Logistics

     a. Recommendations for changes to this Order should be submitted to the IP Branch, MCICOM G-3.

     b. Reports. All reporting requirements are listed in enclosures (2) through (10).

     c. Logistics. N/A.

5. Command and Signal

     a. Command. This Order is applicable to MCICOM HQ and all MCICOM regional commands.

     b. Signal

          (1) Current Systems. MCICOM will share information primarily via the following systems:

               (a) WEBEOC will be used for maintaining a Common Operating Picture (COP) during emergency situations.

               (b) C4I Suite will be used at all times to disseminate threat information. C4I Suite URL on NIPRNET: https://c4isuite.atfp.cnic.navy.mil/usmc/pages/index.aspx; on SIPRNET: https://c4isuite.atfp.cnic.navy.smil; training site on NIPRNET: https://c4isuite.atfp.cnic.navy.mil/usmc/training/index.aspx. C4I Suite Helpdesk may be reached at (888)-264-4255.

               (c) All assessment data and reports associated with enclosures (2-10) shall be posted to Marine Corps Critical Asset Management System - Next Generation (MCCAMS-NG) per reference (q).

          (2) The MCICOM Watch Officer may be reached via commercial at (571)256-8194, DSN at 226-8194, Blackberry at (910)391-4419, or e-mail at mcicom watch officer.fct@usmc.mil.

          (3) This Order is effective the date signed.

                              J. G. AYALA

DISTRIBUTION: C

1. This enclosure provides information on management of IP programs and resources as a portfolio to support the intent of reference (i). While Service-level policy and procedures for Capability Portfolio Management (CPM) continue to mature, MCICOM is taking steps regarding the organization, PPBE activities, and execution of IP's mission to support CPM. The information in this enclosure is not intended to change or detract from formal guidance on resource management provided by MCICOM G-8 or other offices with primary fiduciary responsibilities.

2. Figure 1.1 is a multi-purpose diagram that shows: (1) IP capabilities synchronized with the COLS functions and definitions, (2) a 'resource map' of IP programs to supporting MCPCs, (3) organizational wire diagram for MCICOM HQ and regional IP Branches providing SME and leading program management activities, and (4) the MA-RMP as the process used to synchronize risk management activities across the IP capability portfolio. The eight "major" programs of the IP capability portfolio are identified and subordinated to three sections of the IP Branch.
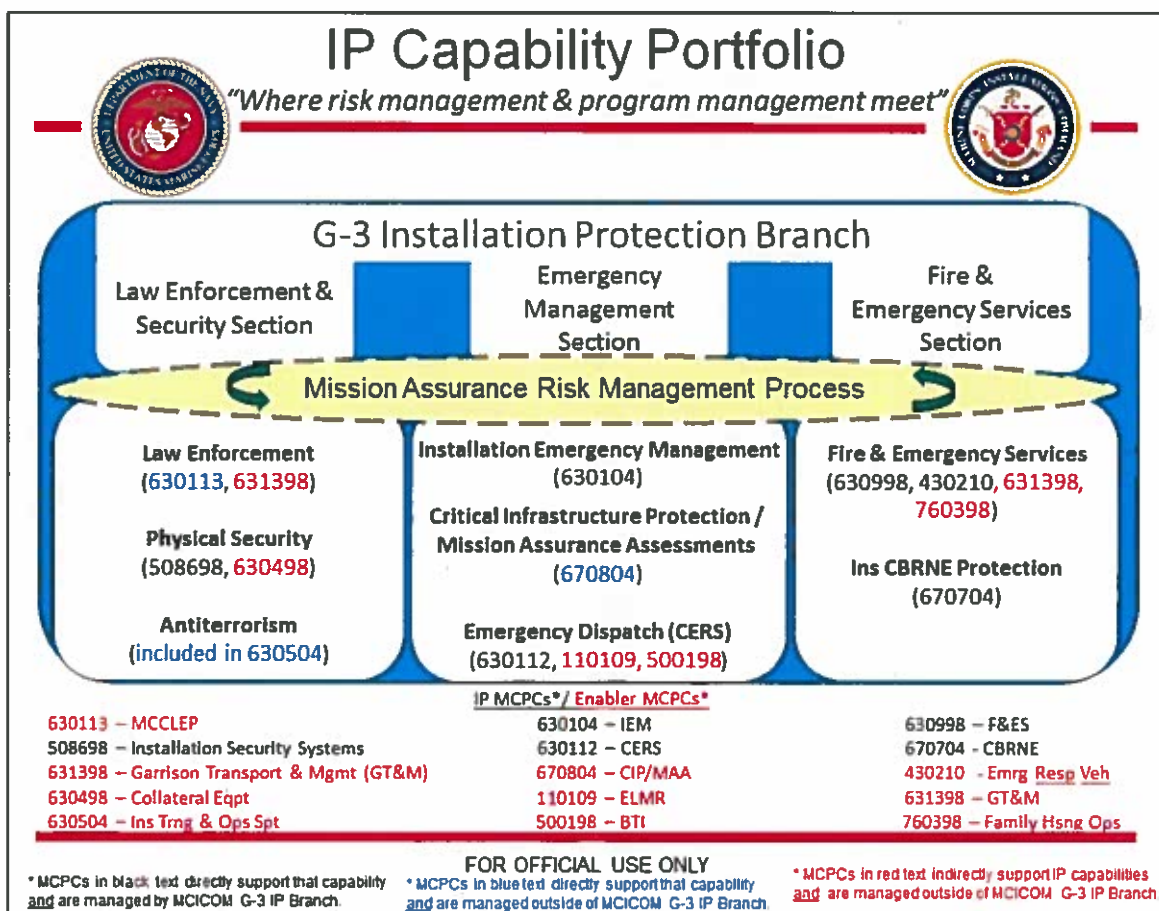

Figure 1.1

Figure 1.1 shows the MCPCs that directly and indirectly resource IP capabilities. MCPCs in black text directly support that capability and are managed by MCICOM G-3 IP Branch. MCPCs in blue text directly support that capability and are managed outside MCICOM G-3 IP Branch. MCPCs in red text indirectly support IP capabilities and/or are managed outside the G-3 IP Branch.

3. COLS are standardized, output-based, and tiered performance levels for accomplishing installation functions. COLS development is led by MCICOM G-5 (Business Performance Office). MCICOM's IP Branch is supporting development of IP-related COLS. The benefits of COLS are captured in Figure 1.2.

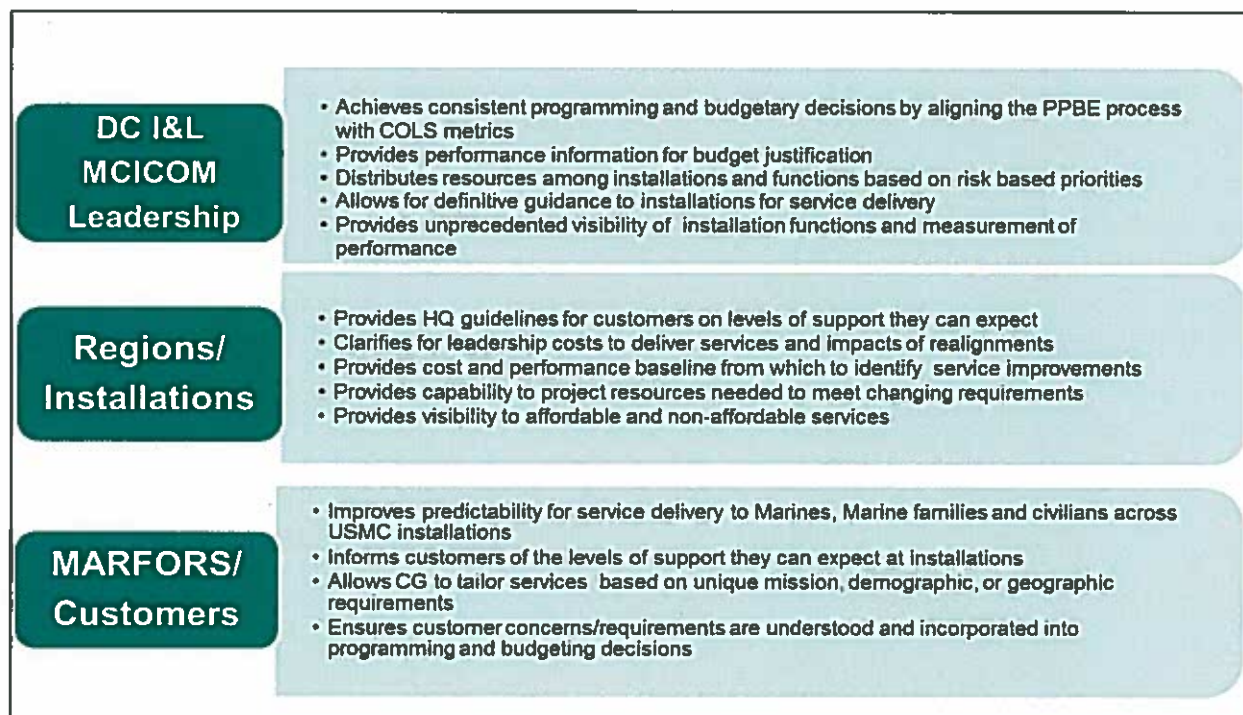| DC I&L MCICOM Leadership	• Achieves consistent programming and budgetary decisions by aligning the PPBE process with COLS metrics • Provides performance information for budget justification • Distributes resources among installations and functions based on risk based priorities • Allows for definitive guidance to installations for service delivery • Provides unprecedented visibility of installation functions and measurement of performance
Regions/ Installations	• Provides HQ guidelines for customers on levels of support they can expect • Clarifies for leadership costs to deliver services and impacts of realignments • Provides cost and performance baseline from which to identify service improvements • Provides capability to project resources needed to meet changing requirements • Provides visibility to affordable and non-affordable services
MARFORS/ Customers	• Improves predictability for service delivery to Marines, Marine families and civilians across USMC installations • Informs customers of the levels of support they can expect at installations • Allows CG to tailor services based on unique mission, demographic, or geographic requirements • Ensures customer concerns/requirements are understood and incorporated into programming and budgeting decisions

Figure 1.2

4. Formal programming guidance comes from MCICOM G-8. Figure 1.3 identifies the IP-related programs aligned to the supporting MCPCs (Figure 1.1) and the COLS-related functions and sub-functions as well as the responsible PM from MCICOM's IP Branch. The figure is information only and is intended to assist regions in identifying the appropriate MCPC for programming IP-related requirements. The 'MCPC descriptions' provided are generic in nature, are not exclusive, and are only intended to assist personnel in identifying the appropriate MCPC for programming IP-related requirements.

MCPC	MCPC Description	COLS Fx	COLS SubFx	PM, MCICOM G-3
630113 – Supporting Establishment Law Enforcement (SELE)	Includes labor funds for civilian police officers and physical security specialists. Non-labor funds provide contractors, equipment, training, services, M&S. Funds also support crime prevention, pre-trial confinement, accident investigation, criminal investigation, violence prevention, and physical security services.	Installation LE and Security	1) PMO Operations 2) PMO Services 3) Criminal Investigation 4) Pre-trial Confinement	LE Section Head - P LE Program Mgr - A
508698 - Installation Security Systems	Includes non-labor funds only; funds the MCESS program (Inclusive of equipment, program mgmt, project eng, 24/7 maint support, etc) Supports physical security training.	N/A	N/A	Physical Sec PM - P LE/Sec Section Head - A
630104 - Installation Emergency Management (EM)	Includes labor for EM/MA/S&ES personnel; Non-labor funds support plan development, training and exercise support, equipment, and technology ISO AH&T-based EM program. Funds MNS/COP systems and supports EOC capability.	EM and CIP	1) Preparedness 2) Response 3) Recovery	EM Section Head - P IP Branch Head - A
630112 - Consolidated Emergency Response System (CERS)/ Emergency Dispatch Services	Acquisition program fielding hardware/software for enhanced 911 and emergency dispatch systems. Also includes labor funds for emergency dispatchers and alarm monitors. Non-labor funds support dispatcher training, certification, equipment, M&S, and sustainment of CERS.	Emergency Dispatch	Emergency Dispatch	EM Comm Spec - P EM Section Head - A
630998 - Fire Protection & Emergency Services	Includes labor funds for firefighters and paramedics; Non-labor funds support training, certification, equipment ISO response to AH. Funds also support fire prevention, fire protection systems IT&M, and fire investigation capabilities.	Fire Protection & Emergency Services	1) Fire, Technical Rescue Hazardous Materials Response 2) Emergency Medical Svcs 3) F&ES Training 4) Fire Prevention 5) Fire Protection Systems Inspection, Testing and Maintenance	F&ES Section Head - P F&ES Program Mgr - A
670704 - Installation Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive (CBRNE) Protection	Includes labor and non-labor funds ISO installation CBRNE protection. Funds training, exercise support, detection and sampling capability, equipment for first responders (including lifecycle support).	CBRNE	1) Equipment 2) Response Planning, Training and Exercises	CBRNE Chief - P F&ES Section Head - A

Figure 1.3

5. Advocacy is important to successful CPM. When IP-related capability/resource gaps are identified through application of risk assessment and analysis, but require resources in excess of MCICOM funding authority, the advocacy construct is used to pursue required means. Figure 1.4 provides a general description of the advocacy bodies that support IP CPM.
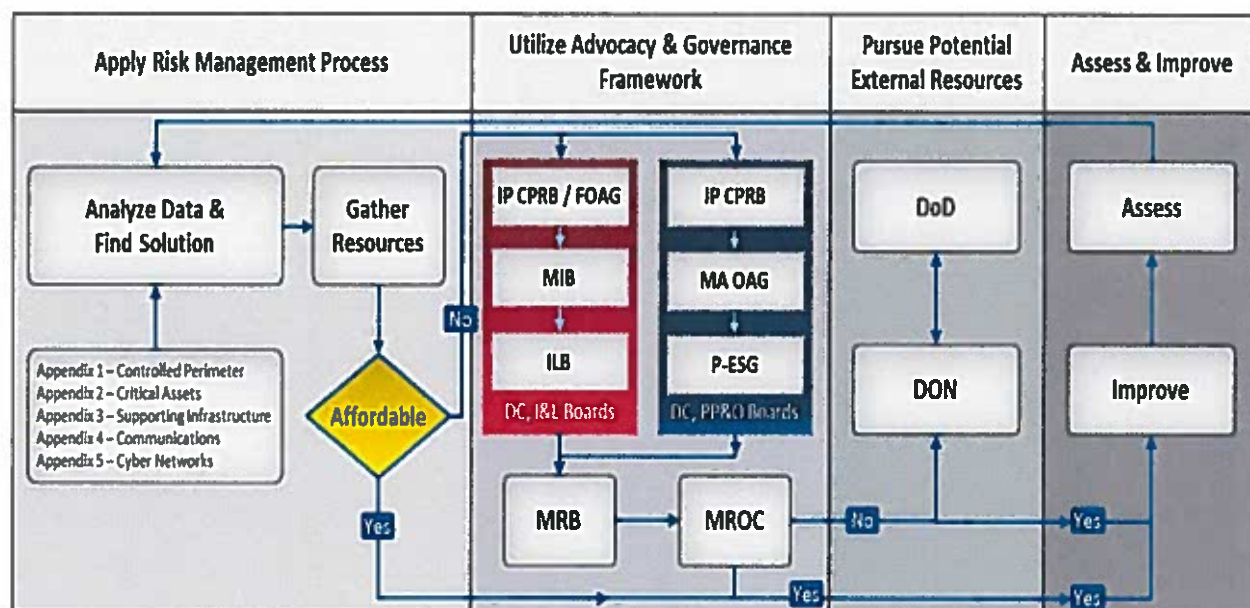
Figure 1.4

MCICOM will begin the process of prioritizing risk and required resources within its own advocacy constructs. All levels of command will use MC-CAMS NG to document risk and identify those needed resources to mitigate the commander's unacceptable level of risk. At the regional level, MAWGs are charged with prioritizing recommendations using a diverse group of experts from across the command's staff to improve the IP capabilities aboard each base and station. Through the IP CPRB, MCICOM will prioritize recommendations across the entire command. TECOM will prioritize recommendations across its SLTIs and forward those recommendations to the MIB via the IP CPRB.

The Marine Installations Board (MIB) will approve solutions or forward recommendations to the appropriate bodies via the Installation and Logistics Board (ILB), chartered and chaired by the Deputy Commandant, Installations and Logistics (DC, I&L), for endorsement. If necessary, IP-related deficiencies are then elevated to the Marine Requirements Oversight Council (MROC) via DC, I&L, where senior Marine Corps leaders can determine Service-wide prioritization and apply available resources. When requirements exceed I&L's funding authority, recommended solutions will also be moved through a parallel path of advocacy boards and oversight councils under the Protection Advocate's (DC, PP&O) construct.

6. Combatant Commander Initiative Fund (CCIF). Emergency or emergent requirements can be submitted for funding under CCIF. CCIF is a limited Joint funding source and receives final

approval by the Joint Staff. The USMC Service Command submissions must compete with submissions from other Services as well as DoD agencies/activities. Requirements must be clearly articulated, fully justified, and thoroughly staffed before being submitted to the CG, MCICOM, via the IPCRB process. Submissions must be recorded in MCCAMS-NG in order to inform the respective COCOM via MARFORPAC or MARFORNORTH.

1. Per reference (d), Mission Assurance (MA) is a uniform, mission-focused process for identifying and managing risk to critical assets that support the execution of Marine Corps operational force and supporting establishment missions, core functions, and capabilities. This enclosure provides guidance and outlines standard procedures for implementation of MA, inclusive of a consolidated mission assurance assessment methodology and forums for risk management that support the overall MA process. This enclosure addresses the risk management process (RMP), MAAs, and MAWGs and attempts to link these components into IP program management activities. Linking the data and products derived from the MA process is essential to enabling risk-informed decision making and justification of resources for IP.

    a. The MA-RMP is rooted in and is essential to the Marine Corps Critical Infrastructure Protection (MCCIP) program. This process ensures "mission owners" and "asset owners" are engaged in a common effort to identify and manage risk to assets and supporting infrastructure that are critical to accomplishing assigned missions.

    b. MAAs are a part of the RMP and include a mission analysis segment that is essential to identification and documentation of critical assets and infrastructure. MAAs also serve to align and synchronize the management of protection-related risk across the Marine Corps by consolidating numerous on-site assessments requirements under one coordinate effort. MAAs consolidate and synergize risk assessment activities required of each protection-related program.

    c. Beginning at the base and station level, protection-related risk is analyzed and recommendations are formed and prioritized via MAWGs. Region-led MAWGs continue to assess and analyze risk and prioritize remediation efforts for their AOR (CG, TECOM prioritizes remediation efforts for its SLTIs). At the MCICOM HQ level, the IP CPRB fulfills the command's MAWG mission. The IP CPRB assesses and analyzes risk and prioritizes remediation efforts for all bases and stations. Risk that cannot be sufficiently addressed at the MCICOM HQ level is then moved into the advocacy construct via the IP CPRB.

2. MA-RMP. Risk Management involves the application of a standardized process to identify, assess, and manage risk and enable decision making that balances risk and cost with mission benefits. RM allows commanders to decide how best to employ allocated resources to reduce risk or, where circumstances

warrant, acknowledge risk. RM consists of two core activities:
Risk Assessment (RA) and Risk Planning (RP).

a. RA involves the collection and evaluation of data
concerning asset criticality based on mission impacts, probable
threats and hazards, and degree of vulnerability to determine
the overall risk posture of the asset. A RA involves the
collection and evaluation of data in three core areas:

(1) Criticality Assessment (CA)

(2) All Hazards Threat Assessment (AHTA)

(3) Vulnerability Assessment (VA)

b. RP is the process of determining options or courses of
action (COAs) to reduce the risk of loss or degradation to the
asset/capability and thus reduce impact to mission execution.
Installation commanders shall implement effective and efficient
risk reduction COA whenever possible. Planners shall make full
use of their Capability Assessment (CA) when developing courses
of action that will rely on the Command's response capabilities
as an integral part of the risk reduction plan.

3. <u>MA Assessments</u>. There are three primary assessments
(described below) that are led by HQMC that together form the
foundation of the consolidated MAA. The MAA is conducted at
each Marine Corps base and station every three years:

a. <u>Marine Corps Mission Assurance Assessment (MCMAA)</u>.
MCMAA is a standard process for assessing and managing risk to
critical assets and infrastructure that directly support Marine
Corps operating forces and supporting establishment missions,
core functions, and related capabilities. The MCMAA is
essential to the MCCIP and is the primary assessment vehicle for
protection-related programs in the IP capability portfolio aside
from F&ES and LE. PP&O (PSM) is the lead office at HQMC with
responsibility for managing the MCMAA.

b. <u>F&ES Program Management Assessment</u>. F&ES program
management assessments provide a detailed analysis and
evaluation of base and station F&ES department programs, mission
capability, and status of each department's self-assessments
efforts using the Commission on Fire Accreditation International
(CFAI) Self-Assessment Manual. I&L (LF) / MCICOM G-3 are the
lead offices at HQMC with responsibility for managing the F&ES
assessments.

   c. Marine Corps Law Enforcement Accreditation Program
(MCLEAP). MCLEAP is a comprehensive evaluation process designed
to assist Provost Marshal Offices (PMOs) and Marine Corps Police
Departments (MCPDs) in improving the quality of law enforcement
support at bases and stations. MCLEAP is a cradle-to-grave
performance improvement process that partners PMOs/MCPDs with
HHQ's to overcome obstacles impacting law enforcement
operations. PP&O (PSL) is the lead office at HQMC with
responsibility for managing the MCLEAP.

4. Post-Assessment Activities. After each consolidated MAA,
reports are released by the cognizant office at HQMC and the
following actions occur:

   a. The reports are posted in MC-CAMS NG with a template
MAP. Bases and stations receive notice of the report via the
chain of command with a suspense date of 90 days from the report
release date. Bases and stations shall thoroughly review each
report and populate the MAP.

   b. Within 90 days of each assessment report's (MA, F&ES,
and MCLEAP) release date, the base and station will deliver the
populated MAP to the Regional Commander. Regional commands are
authorized to share reports and MAP data with supported
commands.

   c. Within 120 days of each assessment report's (MA, F&ES,
and MCLEAP) release date, the region's AC/S, G-3/5 presents a
post-assessment brief to the AC/S, G-3/5/7, MCICOM. The purpose
of the brief is to:

      (1) Maintain oversight of a base and station's progress
in addressing all report recommendations via the MAP.

      (2) Allow regional commands to provide endorsement on
each's prioritization of risk and remediation actions. To
ensure compliance with combatant commander requirements (e.g.
NORTHCOM, PACOM), regional command's shall identify the top 10
areas of protection-related risk for each base and station
within the MAP.

      (3) Allow regional commands an opportunity to identify
and advocate for resources required to complete remediation
activities.

   d. MCICOM will share reports and MAP data as required in
order to meet supported commander's requirements.

5. Obtaining Resources. This section gives guidance on using data and outputs of the MA-RMP and MAAs to gain resources necessary to reduce risk.

    a. Risk Decision Packages (RDP). The primary means to obtain resources to reduce vulnerabilities and eliminate gaps identified by MCMAA is via the RDP. RDPs present one or more COA designed to address and reduce identified risk to critical assets and infrastructure or reduce capability gaps identified within each protection-related program. RDPs are developed to assist commanders in risk decision making.

        (1) The RDP shall include details concerning the asset/capability, specific threats and hazards to which the asset is vulnerable, information concerning the command's decision to reduce risk, and resource requirements needed to execute the plan.

        (2) Installation commanders have several options in handling RDPs. Risk can be acknowledged, solutions can be locally funded, or risk can be reduced by implementing remediation measures. Additionally, a RDP can be forwarded to the regional command or MCICOM HQ for funding or other consideration.

        (3) Before a RDP is forwarded to the regional command or MCICOM HQ, commanders shall prioritize proposed risk reduction COAs.

        (4) If an installation or regional command is unable to fund the selected RDP COA, the RDP shall be forwarded to the appropriate MCICOM G-3 IP Branch PM and a request for a brief shall be made. After being briefed, MCICOM will decide on a COA and resource a solution if applicable. MCICOM will coordinate with CG, TECOM for decisions impacting SLTIs. If resources are not available, MCICOM G-3 will move the requirement to the MCICOM G-8 Current Year Deficiency (CYD) database or into the POM. (NOTE: CYDs can be entered at any point in time, starting at the base and station-level. Regions/Base and stations shall notify the applicable MCICOM G-3, IP Branch PM, if the CYD already exists.)

        (5) Annually, at the start of the fiscal year, RDPs shall be reviewed by the base and station from which it originated. The review of each RDP will validate that the risk still exists and that the selected COA is still appropriate. MCICOM shall receive an updated list of RDPs from each region by

31 January IOT update the CYD database and support the mid-year review.

(6) RDPs shall be documented in MC-CAMS NG for all Tier I-III critical assets at a minimum. Regions shall notify MCICOM G-3 via NIPR e-mail any time action is required on a RDP located on SIPR.

b. <u>F&ES Assessment and Accreditation Reports.</u> The primary means to obtain resources to reduce vulnerabilities and eliminate gaps identified by F&ES Program Management Assessments is through the installation's annual budget, annual CYD funding, or via the POM. F&ES program management has been aligned to the CFAI accreditation model, which is the preferred means to validate F&ES program capability and manage efforts to improve. The model uses a series of performance indicators, grouped by category, which MCICOM has incorporated into F&ES program management activities, including the COLS construct.

(1) When an F&ES report identifies a deficiency, installation commanders have several options. Risk can be acknowledged by a written deviation, solutions can be locally funded, or resource requests can be elevated through the chain of command.

(2) Before a deviation and/or resource request is forwarded to the regional command or MCICOM HQ, commanders shall prioritize proposed risk reduction COAs.

(3) If a base and station or regional command is unable to fund a resource request, the resource request shall be forwarded to MCICOM G-3 (F&ES PM) and a request for a brief shall be made. After the brief, MCICOM will decide on a COA and resource a solution if applicable. MCICOM will coordinate with CG, TECOM for decisions impacting SLTIs. If resources are not available, MCICOM G-3 (F&ES PM) will move the requirement to the MCICOM G-8 CYD database and/or into the POM. (NOTE: CYDs can be entered at any point in time, starting at the base and station-level. Regions/Base and stations shall notify the MCICOM G-3 F&ES PM if the CYD already exists.)

(4) Annually, in conjunction with the CFAI self-assessment, base and station F&ES departments will review outstanding resource requests and validate that the risk still exists and that the selected COA is still appropriate. MCICOM shall receive an updated list of resource requests from each region as part of the annual self-assessment reporting process.

(5) Valid requirements that still exist may be addressed as part of the annual "P-1" centrally managed program (CMP) data call (August-September timeframe). Requirements may also be entered into the CYD database at the base and station level and elevated through the G-8 mid-year review process. MCICOM G-3 (F&ES PM), in coordination with regional F&ES PMs, will prioritize F&ES CYDs for the command.

(6) Enduring requirements not addressed by annual budgets or CYD requests shall be moved into the POM process by the MCICOM G-3 F&ES PM. Trend data from F&ES Assessment and Accreditation Reports and base and station F&ES department strategic plans shall be used to inform the F&ES POM initiative.

c. <u>LE Assessment and Accreditation Reports</u>. The primary means to obtain resources to reduce vulnerabilities and eliminate gaps identified by LE Assessments and the MCLEAP is through the base and station's annual budget, annual CYD funding, or via the POM. LE program management has been aligned to COLS and uses the MCLEAP accreditation model as the means to validate LE program capability and implement continuous process improvement.

(1) When an LE assessment report identifies a capability gap or related deficiency, installation commanders have several options. Risk can be acknowledged, solutions can be locally funded, or resource request can be elevated through the chain of command.

(2) Before a resource request is forwarded to the regional command or MCICOM HQ, commanders shall prioritize proposed risk reduction COAs.

(3) If a base and station or regional command is unable to fund a resource request, the resource request shall be forwarded to MCICOM G-3 (LE PM) and a request for a brief shall be made. After the brief, MCICOM will decide on a COA and resource a solution if applicable. MCICOM will coordinate with CG, TECOM for decisions impacting SLTIs. If resources are not available, MCICOM G-3 (LE PM) will move the requirement to the MCICOM G-8 CYD database and/or into the POM. (NOTE: CYDs can be entered at any point in time, starting at the installation-level. Regions/Base and stations shall notify the MCICOM G-3 LE PM if the CYD already exists.)

(4) Annually, in conjunction with the MCLEAP self-assessment, base and station PMOs/MCPDs will review outstanding

resource requests, validate that the requirement still exists, and confirm the selected COA is still appropriate. MCICOM shall receive an updated list of resource requests from each region by 31 January IOT update the CYD database and support the mid-year review.

      (5) Enduring requirements, not addressed by annual budgets or CYD requests, shall be moved into the POM process by the MCICOM G-3 LE PM. Trend data from MCLEAP Assessment and Accreditation Reports and base and station PMO/MCPD strategic plans shall be used to inform the LE POM initiative.

5. <u>MAWGs/MAECs</u>. To support RM procedures outlined in this enclosure, commands shall establish MAWGs/MAECs. The MAWG is an interdisciplinary body that provides recommendations regarding protection capabilities, gaps, trends, and priorities across individual program elements based upon outputs from the assessments outlined above. The MAWGs influence prioritization of resource requirements (e.g. CYDs, RDPs, and POM) for their commands. MAECs are an executive-level body similar to the MAWG that assesses, integrates, and synchronizes protection-focused capabilities, programs, and resource investments. The MAEC provides a single, multi-disciplinary entity to review IP-related risk, recommend changes, and resource priorities.

    a. Data and outputs of the MA process used by MAWGs/MAECs will help MCICOM achieve the following service goals:

      (1) Mission analysis and RA activities are aligned, synchronized, and uniformly implemented across protection-related programs and activities command-wide.

      (2) Inputs from a unified assessment process inform decision making, resource prioritization, and RM activities at all levels of MCICOM.

      (3) Coordination and synchronization are enhanced between MCICOM and other external stakeholders and partners identified in the Order in protection-related programs and activities.

Law Enforcement

1. Per references (r) and (s), establish a LE Program that is mutually supporting of the overall IP mission to ensure proper enforcement of laws and regulations and protection and safety of personnel.

2. Tasks to Commanding Generals, Marine Corps Installations Pacific, West, East, and National Capital Region

    a. Ensure an LE Program is enacted in order to:

        (1) Enhance safety, protect life, and enforce laws and regulations.

        (2) Protect critical assets and infrastructure aboard the bases and stations that are vital to mission execution.

        (3) Ensure continued operation of mission critical/essential functions and respond to AH&T incidents.

    b. Assign and designate in writing a Regional LE Program Manager.

    c. Identify required resources to establish, maintain, and execute a LE/security activities supportive of the installations AH&T EMP and consistent with missions supported; critical assets/infrastructure supporting mission execution; and threat, vulnerability, and risk assessments.

    d. Establish and maintain MOUs/MOAs with Federal, State, local, tribal, and HN authorities and/or LE organizations pursuant to all applicable DOD rules, regulations, and policies.

    e. Coordinate with supported MEF Commander to ensure:

        (1) MOU/MOA/Fleet Assistance Program (FAP) supporting installation law enforcement and security requirements are being met per CMC guidance.

        (2) LE personnel supporting MOU/MOA/FAP agreements are receiving and maintaining required MOS related training before and during assignment.

        (3) Plans to return LE personnel to their respective parent command are maintained and updated to ensure support of operation plans and contingency response.

f. Support AH&T Assessments and risk management process.

g. Support the LE accreditations triennially per applicable formats and HHQ guidance.

h. Coordinate receiving and evaluating criminal information and higher headquarters threat assessments and warnings to ensure the region/base and station is adequately postured to contend with evolving threats.

i. Ensure subordinate commands are in compliance with all LE MAA benchmarks per reference (t). These are the minimum standards for evaluation. Commanders may exceed these requirements.

j. Utilize the Marine Corps LE Accreditation Program (MCLEAP) model for program evaluation and improvement.

k. In conjunction with Naval Criminal Investigative Services (NCIS), compile and maintain a local threat assessment that is specific to the regional's mission, assets, and geographic location.

l. Establish and maintain a security augmentation force in accordance with ref (t) to ensure Marine Corps installations can support and sustain the escalation of FPCONS.

m. Implement Three-Dimensional Policing Model (3DPM) following guidance of DC, PP&O.

3. POC for the MCICOM LE program is the MCICOM G-3 LE PM. The LE PM may be reached at (571)256-8451.

Physical Security

1. Per references (u), (v), and (w), establish a Physical
Security (PS) Program that enhances unit, base, and station
physical security by integrating physical security planning,
requirements, capabilities, and procedures.

2. Tasks to Commanding Generals, Marine Corps Installations
Pacific, West, East, and National Capital Region

    a. Commanders shall integrate regional security efforts to
ensure continuity in providing an effective PS Program that will
achieve the necessary levels of protection of DoD personnel,
including and assets, per references (u), (v), and (w).

    b. Commanders shall apply the principles of the PS Program
per reference (u) and fully integrate them into IP-related plans
to ensure employment of a holistic PS Program that integrates
and synchronizes the following: Detection, Assessment,
Delay/denial, Communication, and Response.

    c. Assign and designate, in writing, a Regional PS Program
Manager.

    d. Test/exercise the PS plan on an annual basis per
reference (l). The test can be conducted in conjunction with
the AH&T Exercises.

    e. Specify actions required for incident response, to
include protections against CBRNE Attacks, (including those
using postal systems), High Risk Personnel (HRP) protection,
barrier plans and facility standoff and coordination with other
emergency services and response and recovery organizations.

    f. Identify required resources to establish, maintain, and
execute a regional PS protection plan aiding and consistent with
protection of critical assets and infrastructure supporting
mission execution.

    g. Support the MA risk management process.

    h. Support the LE accreditations triennially per applicable
formats and HHQ guidance.

    i. Coordinate receiving and evaluating criminal
information, and higher headquarters threat assessments and
warnings, in order to determine their applicability.

j. In conjunction with NCIS, compile and maintain a local threat assessment that is specific to the regional's mission, assets, and geographic location.

k. Ensure subordinate commands meet compliance with all PS MAAT benchmarks per reference (t). These benchmarks address the Mission Assurance/Risk Management Methodology (MA/RMM) per reference (d) and should guide all planning and training activities. These are the minimum standards for evaluation. Commanders may exceed these requirements.

l. In accordance with reference (u), submit a quarterly report that captures all uncorrected/outstanding discrepancies exceeding 90 days that were identified through the Physical Security and Crime Prevention Survey.

m. Conduct quarterly PS Council Meetings/Working Groups with installation representatives in order to enhance communication and overall security posture. This WG may be combined with similar WGs for efficiency.

3. POC for the PS program is the MCICOM G-3 PS PM. The PS PM may be reached at (571)256-8451.

Antiterrorism

1. Per references (b), (j), and (x) establish an
AT Program that provides the foundation to manage risk and
protect Marine Corps assets and personnel.

2. Tasks to Commanding Generals, Marine Corps Installations
Pacific, West, East, and National Capital Region

    a. Ensure an AT program is executed in order to:

        (1) Enhance safety and protect life, as well as
property, by addressing terrorism.

        (2) Protect critical assets and infrastructures vital to
mission execution from terrorism.

    b. Develop and execute an AT program that follows all
applicable references.

    c. Synchronize and align AT requirements with all other
protection-related programs as a part of a regional AH&T EMP.

    d. Ensure that an Antiterrorism Executive Council (ATEC)
and an Antiterrorism Working Group (ATWG) are established,
executed, and meeting minutes are maintained.

    e. Appoint an AT Level II certified Antiterrorism Officer
in writing in accordance with reference (j).

    f. Identify required resources to establish, maintain, and
execute an installation AT Plan with activities consistent with
missions supported; critical assets/infrastructures supporting
mission execution; and threat, criticality, vulnerability, and
risk assessments.

    g. Provide guidance on AT training for DOD personnel,
family members, and contractors hired by DOD. This guidance
should cover Level I, II, and AT training and support
operational requirements. To conduct Level I, computer based
training and instructor based training are available to meet
this requirement. To conduct Level II, mobile training team is
the single source to meet this requirement. Regional Commanders
will ensure that personnel stationed OCONUS receive AT Level I
training within 30 days of arrival in theater, and that this
training includes at a minimum, the terrorist and criminal
threats, FPCONs in the AOR, Geographic COCOM specific AT
requirements, and the COCOM information requirements.

   h. Apply the principles of the AT Program and fully integrate them into EM Plans to ensure employment of a holistic system to counter terrorist capabilities. Regional Commanders will ensure that family members living OCONUS receive AT level I training within 30 days of arrival in theater and annually thereafter until return to CONUS, and that this training includes at a minimum, the terrorist and criminal threats, FPCONs in the AOR, Geographic COCOM specific AT requirements, and the COCOM information requirements.

   i. Adhere to established Marine Forces North (MFN) and Marine Forces Pacific (MFP) policies and procedures for setting FPCON levels; FPCON transition; dissemination and implementation of FPCON measures; notification of higher headquarters and affected DOD component headquarters; development of site-specific FPCON measures; and a waiver (exceptions) process for FPCON implementation (approved waivers shall be in writing, consistent with the guidelines outlines in MFN/MFP policy).

   j. Regions and subordinates shall develop and implement random antiterrorism measures (RAM) as an integral component of the overall AT program.

   k. Coordinate with all relevant organizations and agencies regarding threats to DoD critical assets or national security interests related to the Defense Critical Infrastructure Program (DCIP) for use in providing DCIP risk management support to the Intelligence Community.

   l. Establish the process by which their personnel comply with Geographic Combatant Commander (GCC) theater entrance/transit AT requirements and terrorist threat information. This includes; ensuring PCS personnel receive the theater specific briefs, theater specific requirements are completed for deployments and entered into Aircraft and Personnel Automated Clearance System (APACS), personnel complete other training or actions required by that theater (e.g., SERE 100.1, ISOPREP) and are currently qualified within the designated time frame, and any theater specific briefs provided to regional personnel traveling OCONUS on leave (Foreign Clearance Guide & GCC requirements).

   m. Establish a TWG that meets at least quarterly to develop and refine AHTA and coordinate and disseminate warnings, reports, and summaries.

Antiterrorism

n.   Establish an Antiterrorism Executive Committee (ATEC) that meets at least semi-annually to develop and refine AT program guidance, policy, and standards; to act upon recommendations of the ATWG and TWG; and to determine resource allocation priorities to mitigate or eliminate terrorism-related vulnerabilities. This executive committee can be combined with similar committees.

o.   Ensure the AT program adheres to Mission Assurance Assessment benchmarks per references (t). These are minimum standards; Commanders may exceed these requirements.

p.   Provide guidance and oversight to ensure contracts are written to incorporate AT requirements.

3.   POC for the AT program is the MCICOM G-3 AT PM. The AT PM may be reached at (703)695-0105.

Installation Emergency Management

1. Regional Commanders will execute IEM responsibilities, per this Order and references (f) and (l).

2. Tasks to Commanding Generals, Marine Corps Installations Pacific, West, East, and National Capital Region.

    a. Designate, in writing, an Emergency Manager to perform the duties outlined in this Order and in references (f) and (l).

    b. Direct bases and stations to develop, implement, sustain, and annually review a comprehensive "all-hazards" Emergency Management Plan (EMP), that includes the following:

        (1) Plans must be scalable, flexible, adaptable to local needs, and reflect installation missions, goals, and objectives; and assigned functional roles and responsibilities relating to emergency preparedness activities, as well as response, recovery, and communications planning.

        (2) Plans should be updated based on annual reviews and/or lessons learned during exercises or real-world events.

        (3) For procedures and policies at bases and stations Outside the Continental United States (OCONUS), maintain consistency with National Planning Frameworks, National Incident Management System (NIMS), and guidelines to the greatest degree practical, except where compliance otherwise at such locations is mandated.

        (4) Develop and maintain a comprehensive regional Continuity of Operations (COOP) Plan, per reference (y), that ensures Command Mission Essential Functions (MEFs) continue with little or no interruption during and in the aftermath of an emergency. The regional COOP Plan shall be reviewed and validated annually and coordinated with installation COOP plans; updating plans every year or more frequently as circumstances warrant. The COOP plan shall consider and address CIP requirements as required to make sure Task Critical Assets (TCAs) and Supporting Infrastructure Assets (SICAs) remain operational to preclude mission failure. This includes addressing redundancy, resiliency, security, and diversity of TCAs/SICAs, and by making sure installation support contracts and maintenance funding are prepared to support recovery operations.

        (5) Develop, publish, and assess regional IEM policy and direction, per reference (l), which includes, at a minimum:

(a) Employment of the Marine Corps Mass Notification System.

(b) Maintenance of a Common Operating Picture (COP).

(c) Coordination with Family Assistance Programs in the development of the Emergency Family Assistance Plan and response, for its synchronization into the All Hazards Plan.

(d) Ensure Community Awareness information and emergency preparedness activities are made available to all assigned personnel.

(e) Conduct an annual review, update as required, and exercise Mutual Aid Agreements (MAA), MOA, MOU, and ISSA with Federal, State, Host Nation (i.e. Status of Forces Agreement (SOFA), Foreign Consequence Management (FCM), and Humanitarian Assistance and Disaster Relief (HADR)), local, tribal, other service organizations, and base and station tenant organizations to ensure effective emergency response and recovery.

(f) Execution of notification protocols, both internal (Installation personnel only), and external (with local, State, tribal, other military service(s), and host-nation partners), which include mass warning and notification; command, control and communications; first responders and receivers; response to waterside security threat (if required); emergency operators and specialists; medical response; mass casualty; religious support response; and shelter in place/emergency lockdown.

(g) Establishment of regional and IEM Working Groups (IEMWG) to guide "all-hazards" program planning and resource requirements. Other WGs may be combined with the IEMWG.

<u>1</u>. Include Recovery Working Groups as sub-working groups in the EMWG structure.

<u>2</u>. Develop written Charters for EMWGs defining duties, responsibilities, meeting frequency, and composition. Reference (m) provides the required participants for the EMWG.

<u>3</u>. Per ref (f) maintain a record of minutes for committees, working groups, and councils for a minimum of two years.

(h) Conduct of IEM training and implementation of an annual exercise and evaluation program that includes participation of appropriate leaders and decision makers per references (f), (l), and (z).

(i) Provide effective resource management and oversight to establish, maintain, and execute an IEM program and planning, programming, and budgeting for IEM program requirements. Resource management will maintain proper total life-cycle management of IEM equipment including fielding, storage, and replacement functions.

(j) Coordination of regional policy and guidance with US Navy medical treatment facilities on USMC Installations and the Public Health Emergency Officer (PHEO) for the employment of medical resource management and to ensure Public Health Emergency preparedness, fatality management, and mortuary affairs are integrated into IEM planning.

(k) Commanders shall ensure personnel complete, document, and track required NIMS and National Response Framework (NRF) training and education per reference (f).

(6) Coordinate with supported commands (operating forces/tenants) in order to:

(a) Identify operational and support requirements for the base and station.

(b) Collect input on local policy and directives.

(c) Encourage representation at the installation EMWG.

(d) Support base and station operations through the Fleet Assistance Program.

(e) Support the local community engagement plan.

(f) Provide resources (personnel and/or equipment) in support of the installation's emergency response and recovery operations based on established MOU/MOAs.

(7) Ensure the IEM program maintains compliance with MAA benchmarks per references (t). These are minimum standards; Commanders may exceed these requirements.

(8) Establish any needed Mutual Aid Agreements/MOUs/MOAs with local, state, federal and/or host nation incident response and/or emergency management organizations pursuant to all applicable DOD rules, regulations and policies.

(9) Plan and execute an AH&T-based exercise program consistent with reference (f). Exercises shall include scenarios which support activation and validation installation EMPs. Submit an annual consolidated AH&T-based training and exercise program master plan to MCICOM, IP Branch.

(10) Ensure access to CIP data in Emergency Operations Centers and crisis action centers to support real world events and operations.

3. POC for the IEM program is the MCICOM G-3 IEM PM. The IEM PM may be reached at (703)614-7928.

Critical Infrastructure Protection

1.   Per reference (aa), execute a CIP Program that supports and synchronizes with other IP programs and is supportive of Marine Corps and geographic combatant command requirements (e.g. USNORTHCOM, USPACOM).

2.   Tasks to AC/S, G-3/5/7, MCICOM

    a.   Appoint a Critical Infrastructure Protection Officer, in writing, who will lead the coordination and execution of all CIP requirements per reference (aa).

    b.   Develop, execute, and maintain CIP policy and guidance.

    c.   Verify and validate all assets identified by regional commands in MC-CAMS NG per reference (aa). When there is disagreement on verification/validation, return the asset to the regional command with appropriate justification via MC-CAMS NG.

    d.   Implementation of CIP awareness, education and training, to including MC-CAMS NG Training, includes RM, Critical Asset Identification Process and Marine Corps-Asset Prioritization Methodology e-learning.

3.   Tasks to Commanding Generals, Marine Corps Installations Pacific, West, East, and National Capital Region

    a.   Ensure a CIP program is executed in order to:

        (1) Protect critical assets and infrastructures vital to mission execution.

        (2) Ensure continued operation of mission critical/essential functions and respond to AH&T incidents, to include coordination with owners of infrastructure nodes off bases and stations that may affect a base's and station's ability to conduct its mission.

    b.   Appoint a Critical Infrastructure Protection Officer, in writing, per reference (aa).

    c.   A baseline program will address the following, using the MA-RMP and MC-CAMS NG:

        (1) Identify assets and infrastructures critical to the execution of Marine Corps missions, core functions, and capabilities, whether owned by the Marine Corps, other DoD components, governmental entities, tenants, or the private

sector. HHQ guidance requires COOP plans to identify, integrate and address mitigation of the loss of Tier I-II critical assets and their impact on maintaining continuity of operation.

(2) Conduct AH&T analysis, addressing the full range of probable threats and hazards, both natural and man-made, to assess critical assets.

(3) Conduct risk-based criticality and vulnerability assessments to prioritize critical assets based on impact to assigned missions, core functions, and capabilities if those assets are lost, degraded, or disrupted.

(4) Identify remediation and mitigation options for reducing risk to critical assets and infrastructure, via RDPs. MC-CAMS NG is the authoritative database the Marine Corps uses for managing mission and asset data. At a minimum the following areas will be addressed in the RDP:

(a) Paragraph 1 - (Asset Information) will include the asset name, detailed description of the asset, asset owner, and asset point of contact.

(b) Paragraph 2 - (Asset Impact on Supported Mission) will include a summary of mission impact (Paragraph 2A) and Asset Priority Rating (Paragraph 2B).

(c) Paragraph 3 - (Threat/Hazard Assessments) will reflect all Threats/Hazards rated Critical or High (Paragraph 3A). All sources used in the development of the Threat/Hazards will be listed in Paragraph 3C.

(d) Paragraph 4 - (Asset Vulnerabilities) will include Vulnerability/Threat pairing in Paragraph 4A. A summary of the Vulnerability/Threat pairing that includes the Asset Name, Impact Rating, Vulnerability Rating, and Risk Rating in Paragraph 4B (information obtained from Paragraph 5). All sources used in the vulnerability assessment will be listed in Paragraph 4c.

(e) Paragraph 5 - (Risk Reduction) will include at least two COAs in Paragraph 6A and an estimated cost for each COA in Paragraph 6B.

(f) Paragraph 6 - (Commander Review and Decision) For any decisions deferred to HHQ, must include Directive/Policy

that accurately depicts requirements and the impact on the asset if resources are not provided.

      (5) Provide recommendations to commanders on whether to accept risk or to implement remediation or mitigation options designed to reduce risk of loss to critical assets and infrastructures.

    d. Identify required resources to establish, maintain, and execute Regional CIP program activities consistent with missions supported; critical assets/infrastructures supporting mission execution; and threat, criticality, vulnerability and risk assessments.

    e. Per reference (q), manage the identification, prioritization, and risk management of mission critical assets via MC-CAMS NG, to enter/review, validate, and prioritize base, station, and regional asset information, TCAs, and SICAs.

    f. Increase CIP awareness though information sharing, training and education, and cooperative agreement and outreach with the local commercial and government providers of critical services and infrastructure assets that support Marine Corps missions and core capabilities.

    g. Adhere to the Mission Assurance Assessment Supporting Establishment Commands benchmarks per reference (t). These are the minimum standards for evaluation; Commanders may exceed these requirements.

    h. Direct bases and stations to incorporate requirements for the identification, prioritization, and protection of TCAs and SICAs in facilities-based acquisition, maintenance, and sustainment contracts; and in facility construction, installation recapitalization, and installation-level outsourcing and privatization efforts.

    i. Ensure that contracted operations and maintenance support affecting TCAs or SICAs is covered by Service Level Agreements (SLAs) that contain remediation/mitigation options in the case of an undesirable event.

    j. Ensure and validate that support contracts covering TCAs or SICAs aim to provide continuous and uninterrupted levels of material and services.

4. POC for the CIP program is the MCICOM G-3 CIP PM. The CIP PM may be reached at (703)614-7928.

1. <u>Situation</u>. Enclosure will be provided upon release of the
Marine Corps Order addressing Emergency Dispatch Services.

Fire Protection and Emergency Services

1. Per reference (ab), establish and execute an FP&ES Program that enhances Marine Corps mission capability by protecting bases and stations through preventative risk management, education, emergency response, and risk communication.

2. Tasks to Commanding Generals, Marine Corps Installations Pacific, West, East, and National Capital Region

    a. Implement a comprehensive installation/facility F&ES program per reference (ab) in order to:

        (1) Protect all personnel from risk of death, injury, illness, or property damage.

        (2) Protect critical assets and infrastructures vital to mission execution.

        (3) Ensure continued operation of mission critical/essential functions and respond to all hazards incidents.

        (4) Provide assistance to civil authorities under mutual aid agreements, host nation support agreements, and Defense Support of Civil Authorities.

    b. Designate an F&ES Fire Chief or Fire Protection Specialist to manage the program.

    c. Support HHQ F&ES Program Assessments and Mission Assurance Assessments per reference (g).

    d. Develop an F&ES plan that specifies measures for all hazards response, fire prevention and public fire education, fire protection engineering, training and certification, self-assessment and accreditation, and incident reporting and records management.

    e. Provide effective resource management and oversight necessary to establish, maintain, and execute an installation F&ES program.

    f. Establish and maintain MOUs/MOAs with Federal, State, local, tribal, and HN authorities and/or Fire Protection and Emergency Services organizations pursuant to all applicable DOD rules, regulations, and policies.

g. Coordinate and track F&ES training and certification requirements per references (ab) and (ac).

h. Utilize the CFAI model for program evaluation and improvement per reference (ac).

i. Regional commands must maintain compliance with MAA benchmarks per reference (t). These are the minimum standards for evaluation. Commanders may exceed these requirements.

3. POC for the FP&ES program is the MCICOM G-3 FP&ES PM. The FP&ES PM may be reached at (571)256-7259.

Installation Chemical, Biological, Radiological,
Nuclear and Explosive (CBRNE) Protection

1. All regions will implement a comprehensive CBRNE
preparedness program per references (ad), (ae), and this Order.
As it may not be possible to determine if a CBRNE release was an
accident or a deliberate incident during the initial response
effort, the installation CBRNE Protection Program must include
an all hazards approach.

2. Tasks to Commanding Generals, Marine Corps Installations
Pacific, West, East, and National Capital Region

    a. Implement a regional CBRNE preparedness program per
references (ad), (ae), and this Order to include integration of
DoD CBRNE Emergency Response Guidelines, deployment of CBRNE
sensors and detectors, and providing individual protective
equipment in the following priority: emergency/first
responders, critical personnel, essential personnel and other
personnel not included in previous categories. Regional CBRNE
preparedness will be accomplished through a tiered approach,
utilizing the five areas of CBRNE passive defense: prevention,
protection, mitigation, response, and recovery per reference
(ad).

    b. Maintain CBRNE program oversight of all subordinate
commands, bases and stations.

    c. Ensure information/intelligence requirements address
CBRNE specific issues.

    d. Review and provide input to HHQ CBRNE policy.

    e. Use CBRNE assessment standards/benchmarks per reference
(ad), and incorporate these in installation PRs.

    f. Per reference (p), attend and coordinate with the TWG to
rapidly identify if a CBRNE threat is directed towards a base,
station, or facility.

    g. Ensure CBRNE preparedness is addressed in regional
plans, orders and exercises, to include mission continuity and
the safety and well-being of assigned military personnel,
families, and civilian employees during CBRNE events. Maintain
all records concerning development of CBRNE plans for
administrative requirements.

    h. Identify, document, validate, prioritize and submit to
MCICOM G-3 IP Branch (CBRNE) the resource and maintenance
requirements necessary to ensure installation CBRNE

Installation Chemical, Biological, Radiological,
Nuclear and Explosive (CBRNE) Protection

preparedness. Resource minimum requirements will be established
during the annual Basis of Allocation (BOA) Working Group for
response to CBRNE and HazMat incidents.

    i.   Ensure CBRNE hazard assessments and warning and
reporting requirements to HHQ, adjacent, and subordinate
elements are addressed in information architecture requirements
and development.

    j.   Support the triennial MAA and the installation risk
management process.

    k.   Ensure CBRNE preparedness and response planning and
response guidance is provided with a specific operational
framework for each base and station to include sampling,
packaging and chain of custody. This guidance should ensure
coordination with other Federal, State, local, tribal, and HN
authorities, to include initial coordination with Department of
State for all overseas response activities.

    l.   Designate in writing a Regional CBRNE Protection Officer
(CPO) with program management responsibilities.

    m.   Ensure CBRNE preparedness is incorporated into
comprehensive Installation Emergency Management plans.

    n.   Direct, conduct, supervise, evaluate, and document
annual CBRNE response exercises aboard all regional bases and
stations per references (ad) and (ae).

    o.   Ensure the CBRNE program adheres to Mission Assurance
Assessment benchmarks per reference (t). These are minimum
standards; Commanders may exceed these requirements.

    p.   In the event plume modeling is not available, DTRA reach
back information is available at COMM: (703)767-2118, DSN (312)
427-2118.

3. POC for the CBRNE program is the MCICOM G-3 CBRNE PM. The
CBRNE PM may be reached at (703)614-5704.